(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 806 229**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 03196**

(51) Int Cl[7] : **H 04 L 9/00**, G 07 F 7/08, H 04 L 9/32, G 06 F 17/60

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.03.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 14.09.01 Bulletin 01/37.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SCHNEE MATHIEU* — FR et *DUMOULIN OLIVIER GERARD CLAUDE* — FR.

(72) **Inventeur(s) :** SCHNEE MATHIEU et DUMOULIN OLIVIER GERARD CLAUDE.

(73) **Titulaire(s) :**

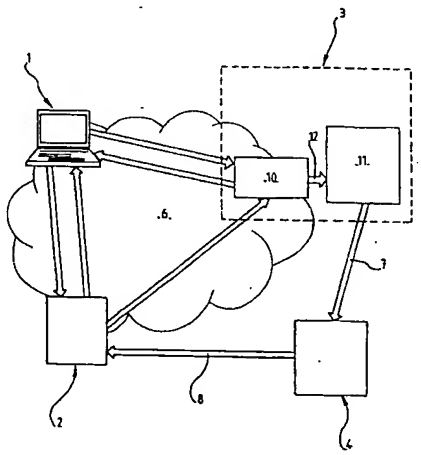
(74) **Mandataire(s) :** CABINET WEINSTEIN.

(54) PROCEDE D'INTERACTION OU DE TRANSACTION ENTRE UN UTILISATEUR ET UN FOURNISSEUR DE PRODUITS OU DE SERVICES ET SYSTEME POUR LA MISE EN OEUVRE DE CE PROCEDE.

(57) L'invention concerne un procédé d'interaction ou de transaction entre un utilisateur et un fournisseur de produits ou services, par l'intermédiaire d'un réseau de transmission de données accessible à des tiers, tel que l'INTERNET.

Ce procédé est du type nécessitant une autorisation préalable, subordonnée à la présentation par l'utilisateur de moyens de preuve de son habilitation, comportant des coordonnées d'habilitation, et à un contrôle de ces coordonnées. Le procédé est caractérisé en ce que l'on fait transiter par le réseau (6) seulement une partie desdites coordonnées, qui à elle seule est insuffisante pour l'autorisation de la fourniture des produits ou services, après avoir mémorisé préalablement l'autre partie dans un organisme intermédiaire de sécurisation (3), et réunit pour ledit contrôle les deux parties de coordonnées.

L'invention est utilisable pour des transactions électroniques bancaires.



FR 2 806 229 - A1

L'invention concerne un procédé d'interaction ou de transaction entre un utilisateur et un fournisseur de produits ou de services, par l'intermédiaire d'un réseau de transmission de données accessible à des tiers, tel que l'INTERNET, du type nécessitant une autorisation préalable, subordonnée à la présentation par l'utilisateur de moyens de preuve de son habilitation, comportant des coordonnées d'habilitation, et à un contrôle de ces coordonnées.

Des procédés de ce type sont connus notamment dans leur application aux transactions électroniques bancaires. L'internet qui progresse d'une façon spectaculaire offre à ces transactions des perspectives d'expansion très favorables. Mais on constate qu'en réalité l'utilisation de ces procédés reste largement en dessous de leur potentiel immense, en raison du manque de fiabilité des réseaux face à la fraude et au piratage. En effet, les procédés de transaction électronique bancaire connus impliquent l'envoi de l'ensemble des coordonnées bancaires, à savoir le numéro de carte et sa date de validité sur le réseau. Bien que l'on ait recours à la cryptographie pour sécuriser les transactions, le risque d'une interception des coordonnées bancaires reste élevé parce que l'arsenal technologique dont disposent les pirates est en perpetuel progrès.

La présente invention a pour but de proposer un procédé de transactions qui pallie les inconvénients des procédés existants.

Pour atteindre ce but, un procédé d'interaction selon l'invention entre un utilisateur et un fournisseur de produits ou services, par l'intermédiaire d'un réseau de transmission de données accessible à des tiers, tel que l'INTERNET, du type nécessitant une autorisation préalable, subordonnée à la présentation par l'utilisateur de moyens de preuve de son habilitation, comportant des coordonnées d'habilitation, et à un contrôle de ces coordonnées, est caractérisé en ce que

l'on fait transiter par le réseau seulement une partie desdites coordonnées, qui à elle seule est insuffisante pour l'autorisation de la fourniture des produits ou services, après avoir mémorisé préalablement l'autre partie dans un organisme intermédiaire de sécurisation, et réunit pour ledit contrôle les deux parties de coordonnées.

Un procédé de transaction selon l'invention entre un consommateur et un site commerçant, par l'intermédiaire d'un réseau de transmission de données, accessible à des tiers, tels que l'INTERNET, à l'aide d'une carte bancaire, du type impliquant un contrôle des coordonnées de carte bancaire par un organisme de contrôle des cartes bancaires, avant l'autorisation de la transaction envisagée, est caractérisé en ce que l'on fait transiter par le réseau seulement une partie des coordonnées de carte bancaire, qui à elle seule est insuffisante pour l'autorisation d'une transaction à l'aide de cette carte, après avoir mémorisé préalablement l'autre partie dans un organisme intermédiaire de sécurisation, que l'on réunit les deux parties des coordonnées de carte bancaire dans cet organisme et fait transmettre les deux parties réunies à l'organisme de contrôle par une ligne de transmission de données non accessible à des tiers.

Le système de transaction électronique entre un consommateur et un site commerçant, par l'intermédiaire d'un réseau de transmission de données public, à l'aide d'une carte bancaire, du type comprenant un organisme de contrôle des coordonnées des cartes bancaires, est caractérisé en ce qu'il comprend un organisme intermédiaire de sécurisation par le stockage d'une partie des coordonnées de carte bancaire, qui est relié au consommateur et au site commerçant par le réseau et à l'organisme de contrôle par une ligne de transmission de données spécialisée non accessible à des tiers, et en ce que l'organisme intermédiaire est adapté pour réunir à la

réception de l'autre partie des coordonnées de carte bancaire reçues par le réseau, les deux parties des coordonnées de carte bancaire et pour transmettre les parties de coordonnées réunies à l'organisme de contrôle par ladite ligne spécialisée.

L'invention sera mieux comprise, et d'autres buts, caractéristiques, détails et avantages de celle-ci apparaîtront plus clairement dans la description explicative qui va suivre, faite en référence à la figure unique annexée donnée uniquement à titre d'exemple et illustrant schématiquement un système de transaction électronique selon la présente invention.

L'invention sera décrite dans son application à un procédé et système de transaction électronique entre un utilisateur-consommateur et un site commerçant.

Sur cette figure unique, les numéros de référence 1, 2, 3, 4 désignent respectivement le consommateur utilisateur, le site de commerce électronique, un organisme intermédiaire de sécurisation des transactions électroniques et l'organisme de contrôle des cartes bancaires. L'utilisateur 1 et le site de commerce 2 sont reliés à un réseau de transmission de données publiques tel par exemple l'INTERNET, indiqué par le numéro de référence général 6 et représenté sous forme d'un nuage gris. On constate que l'organisme de sécurisation 3 est également connecté à ce réseau 6 et peut donc communiquer à travers ce réseau avec l'utilisateur 1 et le site de commerce 2. De plus, l'organisme de sécurisation 3 est relié à l'organisme de contrôle 4 par une liaison de transmission des données spécialisée 7, non accessible à des tierces personnes, telles que par exemple une liaison TRANSPAC. L'organisme de contrôle 4 est susceptible de communiquer avec le site de commerce 2 par une autre liaison spécialisée 8.

Concernant l'organisme de sécurisation 3, il comporte un serveur tampon 10 et un serveur principal 11. Ce dernier comprend une base de données. Les deux

serveurs sont reliés par une liaison de transmission des données interne indiquée en 12.

On décrira ci-après le procédé de transaction électronique selon l'invention, basé sur l'utilisation du système qui vient d'être décrit et qui est représenté, à l'aide d'une carte bancaire et impliquant l'organisme de sécurisation 3.

Pour que l'organisme de sécurisation 3 puisse intervenir, il faut que le consommateur utilisateur 1 se soit préalablement inscrit auprès de cet organisme. A cette fin, l'utilisateur dispose d'une carte d'inscription auprès de l'organisme 3, qui comporte un numéro de série désignant cette carte. Les coordonnées de l'utilisateur, avec le numéro de série de sa carte, sont communiquées par l'utilisateur à l'organisme 3 qui stocke ces coordonnées dans sa base de données contenues dans son serveur principal 11.

Une caractéristique essentielle de l'invention réside dans le fait qu'à la carte d'inscription est associé un code de sécurité qui varie dans le temps selon un algorithme prédéterminé. Ce code est affiché sur la carte. Il est essentiel que l'organisme de sécurisation 3 soit en possession de ce même algorithme de façon à pouvoir connaître à tout moment le code variable s'affichant sur la carte d'inscription de l'utilisateur. Il suffit que ce dernier lui ait communiqué le numéro de série de sa carte lors de son inscription.

L'inscription implique également l'identification de l'utilisateur par un terme l'identifiant, qui pourrait être de toute nature appropriée et comporter les premières lettres de son nom, d'une part, et par un code fixe d'identification, d'autre part. Ce code d'identification fixe est communiqué à l'utilisateur, par l'organisme de sécurité 3, séparément de sa carte d'inscription, et ne figure pas sur la carte. Il est à noter que le code d'identification personnel de l'utilisateur et le code variable sont formés chacun par

exemple par un certain nombre de chiffres. Concernant le code variable, il ne peut pas être reconstitué sans connaissance de l'algorithme et est conçu de façon à changer périodiquement, par exemple toutes les soixante secondes. Selon une autre caractéristique essentielle de l'invention, l'utilisateur communique lors de l'inscription à l'organisme de sécurisation une partie des coordonnées de sa carte bancaire, comportant généralement un numéro de carte et la date de validité. Dans le présent exemple, l'utilisateur communique à l'organisme la date de validité. Cette date sera mémorisée dans la banque de données de l'organisme.

Après s'être inscrit auprès de l'organisme de sécurisation 3, l'utilisateur consommateur est autorisé à effectuer des transactions par exemple des achats par l'intermédiaire de cet organisme. Lorsqu'il souhaite effectuer une transaction sécurisée par l'intervention de cet organisme, il se connecte sur l'un des sites de commerce 2 affiliés et sélectionne les produits ou services de son choix. Au moment de régler ses achats, il indique qu'il a choisi le mode de transaction sécurisée en cliquant sur une icône appropriée apparaissant sur l'une des pages de réglement du site du commerce. Le site commerçant 2 fait alors parvenir à un serveur-tampon 10 de l'organisme de sécurisation 3 des informations précises sur son identité ainsi que celles relatives à la transaction, notamment le montant de la transaction. Dans le même temps, l'organisme de sécurisation 3 génère, à partir des renseignements reçus, un formulaire prérempli à l'attention de l'utilisateur. Ce formulaire indique les références du site commerçant et les informations relatives à la transaction. Si l'utilisateur souhaite poursuivre le processus, il remplit le formulaire en entrant son identifiant et la deuxième partie des coordonnées de carte bancaire, dans le présent exemple le numéro de la carte bancaire.

Lorsque l'utilisateur souhaite ensuite valider le formulaire, il doit s'authentifier en entrant son code d'identification personnel et le code variable s'affichant sur sa carte d'inscription. Ainsi l'ensemble des deux codes constitue un code-passe. Lorsque le formulaire est rempli, une phase d'authentification de l'utilisateur a alors lieu au sein de l'organisme de sécurisation 3, par comparaison des données reçues et des données mémorisées. Si l'utilisateur est identifié et qu'il accepte les termes indiqués sur le formulaire, tel que le montant et les conditions éventuellement spécifiées, une requête est générée dans l'organisme 3 afin de rapatrier des bases de données 11 la date de validité de la carte bancaire enregistrée. Lorsque les deux parties des coordonnées de carte bancaire sont réunies, à savoir la date de validité et le numéro de la carte bancaire, l'organisme 3 transmet l'ensemble des données de transaction, avec les deux parties de coordonnées bancaires réunies, à l'organisme de contrôle des cartes bancaires 4, par la ligne spécialisée 7 qui n'est pas accessible à des tierces personnes. Puis la procédure classique de contrôle a lieu. Le site du commerce et l'utisateur sont informés de l'autorisation ou non de la transaction.

Bien entendu de multiples modifications peuvent être apportées au procédé tel qu'il vient d'être décrit à titre d'exemple. Ainsi l'invention est utilisable avec des cartes bancaires de toute autre nature appropriée. Concernant les coordonnées de carte bancaire, il convient de les séparer en au moins deux parties de façon que la partie qui sera transmise par le réseau soit insuffisante pour obtenir l'autorisation d'une transaction à l'aide de cette carte par l'organisme de contrôle.

Ci-dessus, l'invention a été décrite dans son application à l'achat d'un produit ou d'un service. L'invention peut être en outre utilisée dans tout autre domaine d'interaction ou de transaction où la fourniture

d'un produit ou d'un service nécessite une autorisation préalable, subordonnée à la preuve de la part de l'utilisateur qu'il est habilité à bénéficier de ce produit ou service. Dans certains cas l'organisme de sécurisation pourrait appartenir ou se trouver au site du fournisseur. Par exemple l'invention peut être utilisée pour créer, utiliser, recharger et consulter un compte personnel pour des micropaiements, auprès de l'organisme de sécurisation 3. La création et l'utilisation de ce compte personnel constituant un porte-monnaie électronique se fait également à l'aide de la carte d'inscription sus-mentionnée ou d'une carte du même type. Pour établir ce porte-monnaie, l'utilisateur entre dans des champs d'un formulaire d'établissement du compte son identifiant et le numéro de sa carte bancaire et le montant qu'il désire déposer sur ce compte. Pour valider ensuite la création de ce porte-monnaie électronique, l'utilisateur indique son code-passe comportant son code d'identification personnel et la combinaison variable apparaissant sur sa carte d'inscription.

Lors de l'utilisation de ce compte de porte-monnaie électronique, l'organisme avertira l'utilisateur à chaque fois qu'un paiement fera l'objet d'un prélèvement sur ce compte et lui demandera de s'authentifier par envoi de son identifiant et de son code-passe. L'organisme avertira l'utilisateur également lorsqu'il restera une somme inférieure ou égale à une somme limite prédéterminée ou lorsqu'un achat de faible montant est supérieur à la somme restant sur le compte.

Il est encore à noter que pour éviter un risque de piratage au sein de l'organisme de sécurisation, l'information arrivant par le réseau ne fait pas l'objet d'un stockage.

REVENDICATIONS

1. Procédé d'interaction ou de transaction entre un utilisateur et un fournisseur de produits ou services, par l'intermédiaire d'un réseau de transmission de données accessible à des tiers, tel que l'INTERNET, du type nécessitant une autorisation préalable, subordonnée à la présentation par l'utilisateur de moyens de preuve de son habilitation, comportant des coordonnées d'habilitation, et à un contrôle de ces coordonnées, caractérisé en ce que l'on fait transiter par le réseau (6) seulement une partie desdites coordonnées, qui à elle seule est insuffisante pour l'autorisation de la fourniture des produits ou services, après avoir mémorisé préalablement l'autre partie dans un organisme intermédiaire de sécurisation (3), et réunit pour ledit contrôle les deux parties de coordonnées.

2. Procédé de transaction entre un consommateur et un site commerçant, par l'intermédiaire d'un réseau de transmission de données, accessible à des tiers, tels que l'INTERNET, à l'aide d'une carte bancaire, du type impliquant un contrôle des coordonnées de carte bancaire par un organisme de contrôle des cartes bancaires, avant l'autorisation de la transaction envisagée, caractérisé en ce que l'on fait transiter par le réseau (6) seulement une partie des coordonnées de carte bancaire, qui à elle seule est insuffisante pour l'autorisation d'une transaction à l'aide de cette carte, après avoir mémorisé préalablement l'autre partie dans un organisme intermédiaire de sécurisation (3), que l'on réunit les deux parties des coordonnées de carte bancaire dans cet organisme et fait transmettre les deux parties réunies à l'organisme de contrôle (4) par une ligne de transmission de données non accessible à des tiers.

3. Procédé selon la revendication 2, caractérisé en ce que l'envoi de l'ensemble des coordonnées de carte bancaire par l'organisme de sécurisation (3) à

l'organisme de contrôle (4) est subordonné à l'authentification de l'utilisateur impliquant l'envoi par l'utilisateur à l'organisme de sécurisation (3) d'un code variable dans le temps.

4. Procédé selon la revendication 3, caractérisé en ce que le consommateur utilisateur possède un support portable, tel qu'une carte d'inscription auprès de l'organisme, qui indique le code variable.

5. Procédé selon la revendication 4, caractérisé en ce que le code variable change selon un algorithme prédéterminé.

6. Procédé selon la revendication 5, caractérisé en ce que la carte d'inscription auprès de l'organisme de sécurisation comporte un élément tel qu'un numéro de série qui définit l'algorithme et en ce que ce numéro est communiqué à l'organisme de sécurisation lors de l'inscription et constitue le moyen d'identification de l'algorithme à cet organisme.

7. Procédé selon l'une des revendications 4 à 6, caractérisé en ce qu'au code variable est associé un code fixe d'identification de l'utilisateur, qui est communiqué à ce dernier séparément de la carte d'inscription.

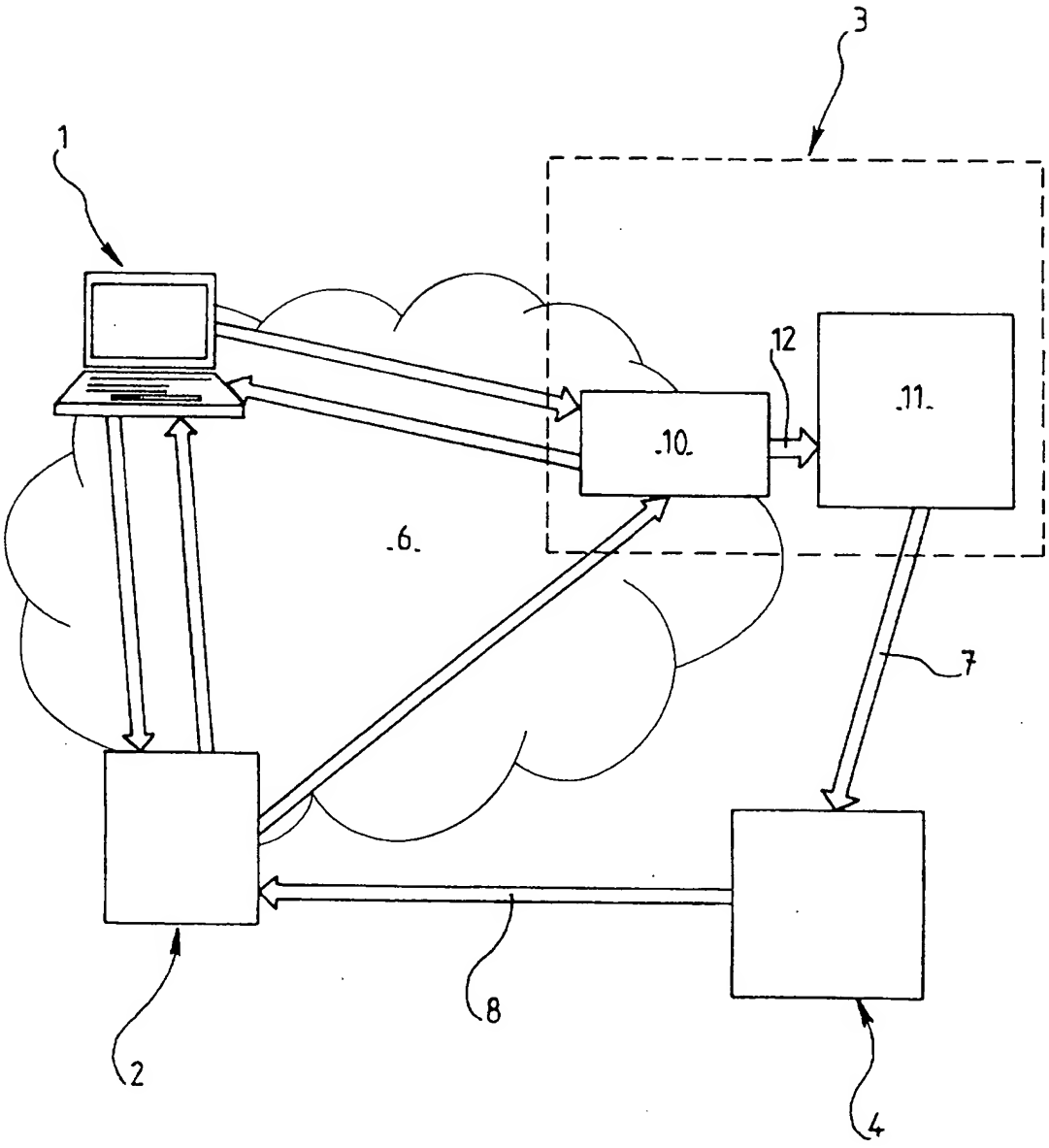
8. Procédé selon la revendication 1, caractérisé en ce qu'il est employé pour la création, l'utilisation, la recharge et la consultation d'un compte personnel pour des micropaiements, le cas échéant auprès de l'organisme de sécurisation.

9. Procédé selon la revendication 8, caractérisé en ce que la création, l'utilisation, la recharge et la consultation du compte de micropaiements sont subordonnées à la présentation par l'utilisation d'un code avantageusement variable.

10. Procédé selon l'une des revendications 1 à 9, caractérisé en ce que les coordonnées qui sont arrives à l'organisme de sécurisation (3) par le réseau précité (6) ne sont pas stockées.

11. Système de transaction électronique entre un consommateur et un site commerçant, par l'intermédiaire d'un réseau de transmission de données accessible à des tiers, tel que l'INTERNET, à l'aide d'une carte bancaire, du type comprenant un organisme de contrôle des coordonnées des cartes bancaires, caractérisé en ce qu'il comprend un organisme intermédiaire (3) de sécurisation par le stockage d'une partie des coordonnées de cartes bancaires, qui est relié au consommateur (1) et au site commerçant (2) par le réseau (6) et à l'organisme de contrôle (4) par une ligne de transmission de données non accessible à des tiers, et en ce que l'organisme intermédiaire (3) est adapté pour réunir à la réception de l'autre partie des coordonnées de cartes bancaires reçues par le réseau (6), les deux parties des coordonnées de cartes bancaires et pour transmettre les parties de coordonnées réunies à l'organisme de contrôle (3) par les lignes spécialisées (7).

12. Système selon la revendication 11, caractérisé en ce que la ligne précitée non accessible à des tiers est une ligne TRANSPAC.


3
1
12
.11.
.10.
.6.
7
8
2
4

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2806229

N° d'enregistrement national

FA 583942
FR 0003196

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 0 855 687 A (AT & T CORP) 29 juillet 1998 (1998-07-29) * page 3, ligne 2 - ligne 4 * * page 7, ligne 42 - ligne 48 * * page 9, alinéa 1 * ---	1,2,11, 12	H04L9/00 G07F7/08 H04L9/32 G06F17/60
A	"AUTHENTICATION WITH STORED KP AND DYNAMIC PAC. OCTOBER 1982" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 25, no. 5, 1 octobre 1982 (1982-10-01), pages 2358-2360, XP002031269 ISSN: 0018-8689 * le document en entier * ---	3-7	
A	US 5 883 810 A (ROSEN DANIEL ET AL) 16 mars 1999 (1999-03-16) * abrégé * * figure 1 * ---	8-10	
A	WO 96 38799 A (AMAZON COM INC) 5 décembre 1996 (1996-12-05) * page 3, ligne 27 - page 4, ligne 10 * * page 7, ligne 20 - ligne 23 * * page 8, ligne 6 - ligne 11 * * revendications 1-3 * ---	1,2,11	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G07F G06F
A	US 5 727 163 A (BEZOS JEFFREY P) 10 mars 1998 (1998-03-10) * colonne 2, ligne 45 - colonne 3, ligne 31 * ---	1,2,11	
A	EP 0 927 945 A (AMAZON COM INC) 7 juillet 1999 (1999-07-07) * colonne 2, ligne 14 - ligne 20 * * alinéa '0007! - alinéa '0008! * --- -/--	1,2,11	

1

Date d'achèvement de la recherche	Examinateur
5 janvier 2001	Wolles, B

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2806229

N° d'enregistrement national

FA 583942
FR 0003196

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 99 44332 A (NAUER BERNHARD ;SIEMENS AG (DE); GUNDLACH MICHAEL (DE)) 2 septembre 1999 (1999-09-02) * page 1, ligne 31 - page 2, ligne 5 * * page 5, ligne 12 - ligne 24 * ---	3-7	
A	US 5 692 132 A (HOGAN EDWARD J) 25 novembre 1997 (1997-11-25) * colonne 3, ligne 21 - colonne 4, ligne 42 * ---	8-10	
A	EP 0 581 689 A (SMART INGENIERIE) 2 février 1994 (1994-02-02) * alinéa '0001! - alinéa '0003! * -----	12	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

1

Date d'achèvement de la recherche	Examinateur
5 janvier 2001	Wolles, B

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)